Windows NT Security Utilities

23 April
1998

Mr. Robert P. Blaisdell
Center for Air Force C² Systems
email: rpb@mitre.org
(781) 271-5757

Background

- HQUSCENTCOM Developed
- Operational Since 1995 (NT3.51 then NT 4.0)
- Augment/Repair Native NT Security Features
- Developed For TS/SCI but Useful to All
- DII AF Sponsoring SECUTL Infrastructure Services Component

What's Being Delivered

- Software Version Description
- Installation Procedures
- User Manual
- System Administrator's Manual
- SECUTL Infrastructure Services Component

What's Not Being Delivered

- Software Requirements Specification
- Software Design Document
- Database Design Document
- Software Test Plan
- Software Test Description
- Software Test Report
- Programmer's Manual
- API Reference Manual

What are the Utilities

- Process Check
- Folder Check
- UNIX Start
- Computer Name
- Event Backup
- NT Print
- Clear Temporary Files
- Log Out

Utility Descriptions and Rational for Use
- Clear Temp

Program:	**Clear temp directory - clrtemp.exe**
Purpose:	**Deletes all files in the temp directory identified by the TEMP environment variable when the user logs off.**
Rational:	**This software directly addresses a Security SRS requirement to remove all temporary files which is not supported in either the NT3.51 or NTv4.0 software.**
SRS Para.s	**3.2.10 Object Reuse**
Description:	**The program is started by using a start command in the logon script. The program will wait until NT sends a WM_QUERYENDSESSION message, at which point all files in the temp directory are deleted**

Utility Descriptions and Rational for Use
- Event Backup

Program:	**Event Backup Service**
Purpose:	**Install and run the event backup service on a Domain Server so that every night at 1 am the service will copy the Security Event Logs from all Domain clients to the Domain Server and then clear them.**
Rational:	**This software directly addresses Security SRS requirements on the maintenance and backup of security audit files that are not directly supported in either the NT3.51 or NTv4.0 software**
SRS Para.s	**3.2.3.1.5 Archive Audit Data**
Description:	**[see chapter 16 in the NT C&I Guide]**

Utility Descriptions and Rational for Use

- Logout on Full Audit Log event

Program:	**logout.exe**
Purpose:	**The logout program is designed to allow only the Administrator to log on if the Security Log is full or if the CrashOnAuditFail key is missing from the Registry.**
Rational:	**This software directly addresses Security SRS requirements on the maintenance and backup of security audit files that are not directly supported in either the NT3.51 or NTv4.0 software.**
SRS Para.s	**3.2.3.1.5 Audit Log Full - response**
Description:	**[see chapter 16 in the NT C&I Guide]**

Utility Descriptions and Rational for Use

- Process Check

Program:	**processcheck.exe, dll**
Purpose:	**Provides the System Administrator a mechanism to restrict the processes that a user can run.**
Rational:	**This software addresses Security SRS requirements to limit or restrict user access to the shell and command line prompts, to control access to restricted programs, directories and files.**
SRS Para.S	**3.2.4.3, 3.2.16. 2/3, 3.2.18 Roles and Profile Management with Object Access**
Description:	**These software modules extend existing Windows NT capabilities included as part of the NT policy editor, and correct NT OS behavior to allow it to conform or meet Security SRS requirements. [see Chapter 16]**

Utility Descriptions and Rational for Use
- Folder Check

Program:	**folderchek.exe**
Purpose:	**Provide System Administrator a mechanism to prevent user access to restricted disk drives.**
Rational:	**This software addresses Security SRS requirements to limit or restrict user access to the shell and command line prompts, to control access to restricted programs, directories and files.**
SRS Para.S	**3.2.4.3, 3.2.16. 2/3, 3.2.18 Roles and Profile Management with Object Access**
Description:	**Foldercheck extends existing an Windows NT capability to “hide drives” included as part of the NT policy editor, and corrects NT behavior to allow it to conform or meet Security SRS requirements. [see chapter 16 in the NT C&I Guide]**

Utility Descriptions and Rational for Use

- Unix Start

Program:	**Unixstart.exe**
Purpose:	**Provides a consistent and simplified UNIX application launch for all NT users. Establishes a mechanism for the system adminstrator to manage a “single logon” capability between UNIX and NT workstations. UNIX password and pass the information to the UNIX box for all X-applications.**
SRS Para.S	**3.2.1.8 Single Sign-on [Best fit]**
Rational:	**This software provides significant simplification and administrative control over the mechanism used to launch UNIX application s for NT Workstations. All control is exercised through the administrator's setup and control of NT registry settings**

Utility Descriptions and Rational for Use

- Computer Name

Program:	cmptrnm.exe
Purpose:	**Provides a secure capability for the user to query the NT registry and identify the computer hostname**
Rational:	**In many secure NT installations user access to the Control Panel applets is restricted. This can make it difficult for the user to determine the machine or host name assigned to the workstation or server. Service or help desk support can be delayed without this information being available.**
SRS Para.S	**3.2.5.13, 3.2.15.3 System Admin and Least Privilege**
Description:	**[see chapter 16 in the NT C&I Guide]**

Utility Descriptions and Rational for Use

- NT Print

Program:	**ntprint.exe**
Purpose:	**Provides Security Headers/Footers**
Rational:	**Print Headers/Footers are required by some agencies.**

DII COE NTAG
DII COE & NT ... Security Utilities
Questions ?

Mr. Robert P. Blaisdell
MITRE ESC/DII
email: rpb@mitre.org
(781) 271-5757